TOOEOF" 206STOOT

Figure 1A

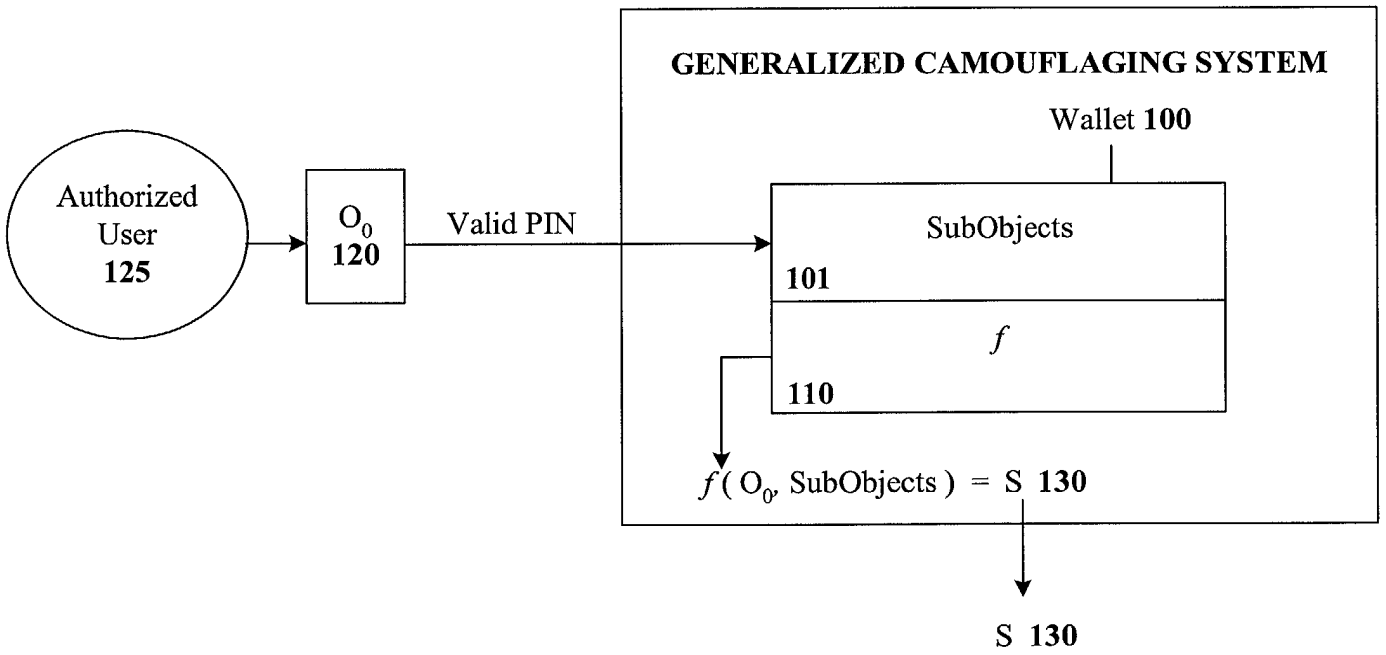


Figure 1B

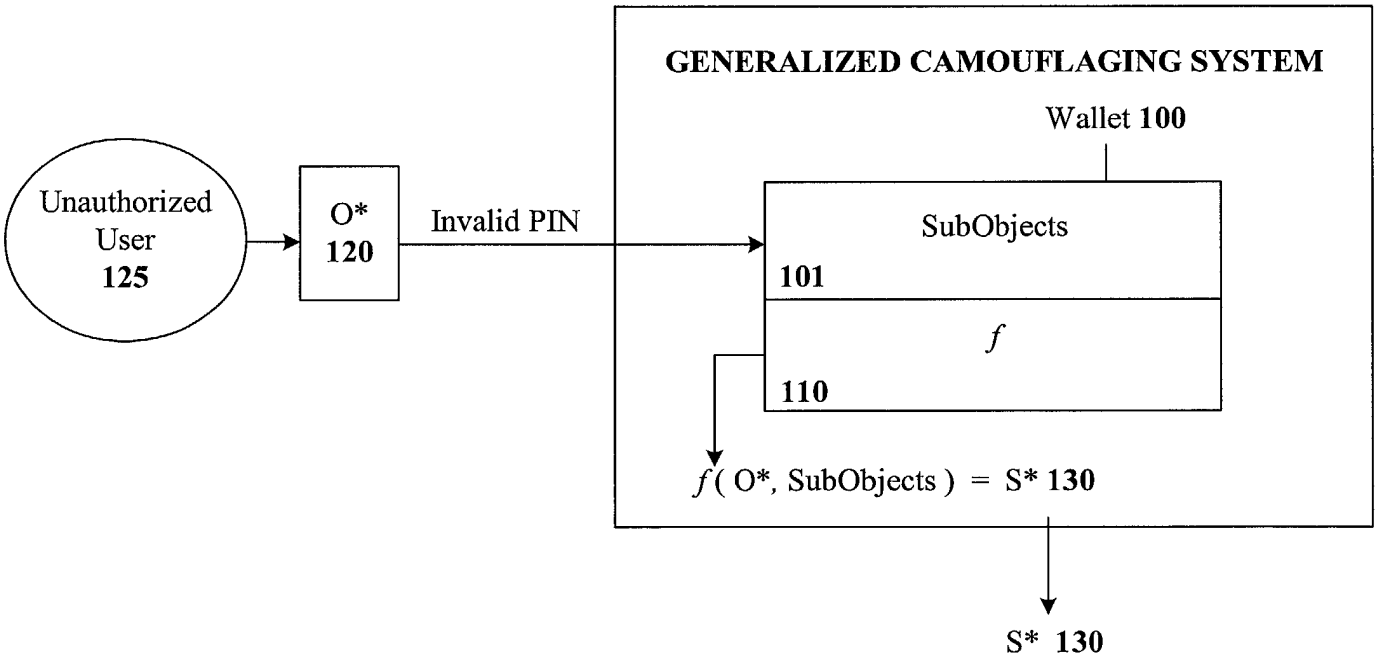

GENERALIZED CAMOUFLAGING SYSTEM
Wallet 100
Unauthorized User 125
O* 120
Invalid PIN
SubObjects
101
f
110
f(O*, SubObjects) = S* 130
S* 130

Figure 2

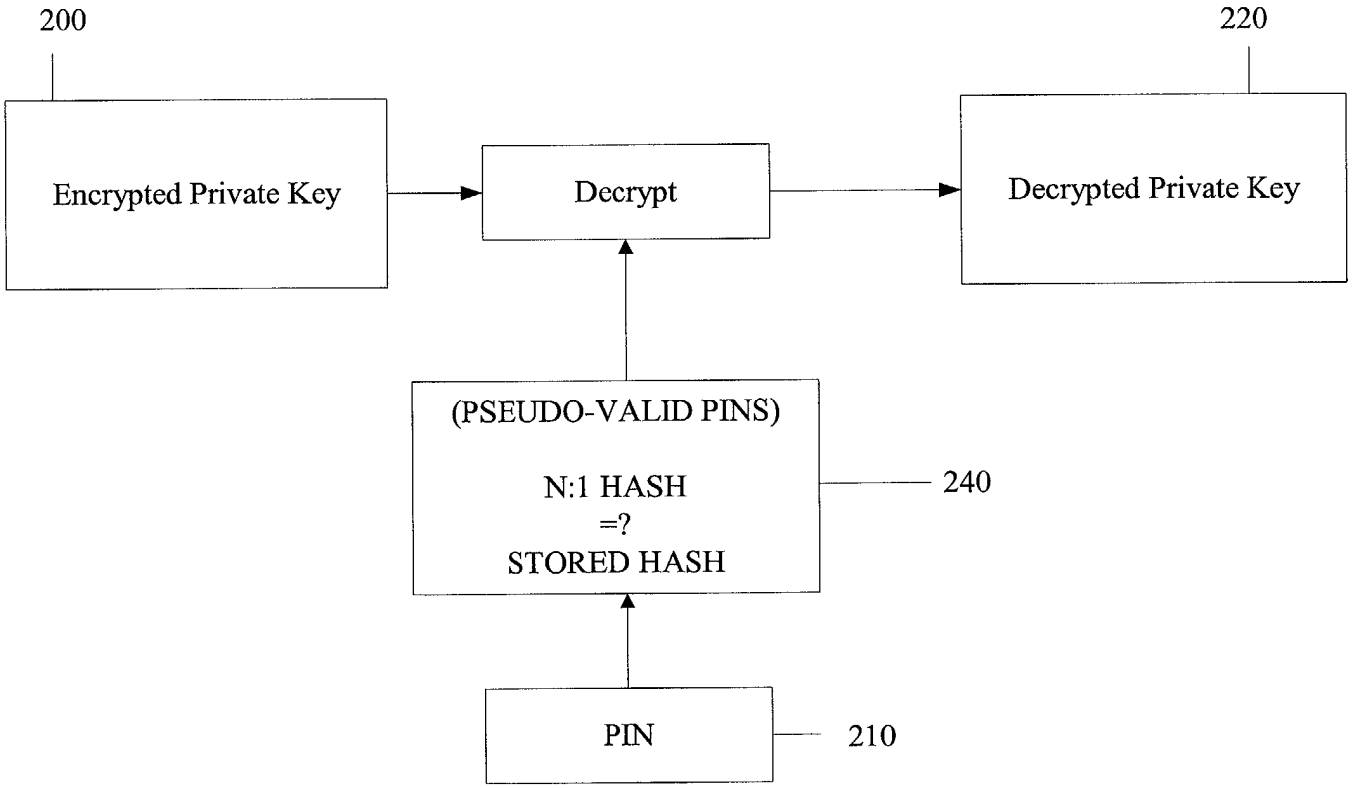
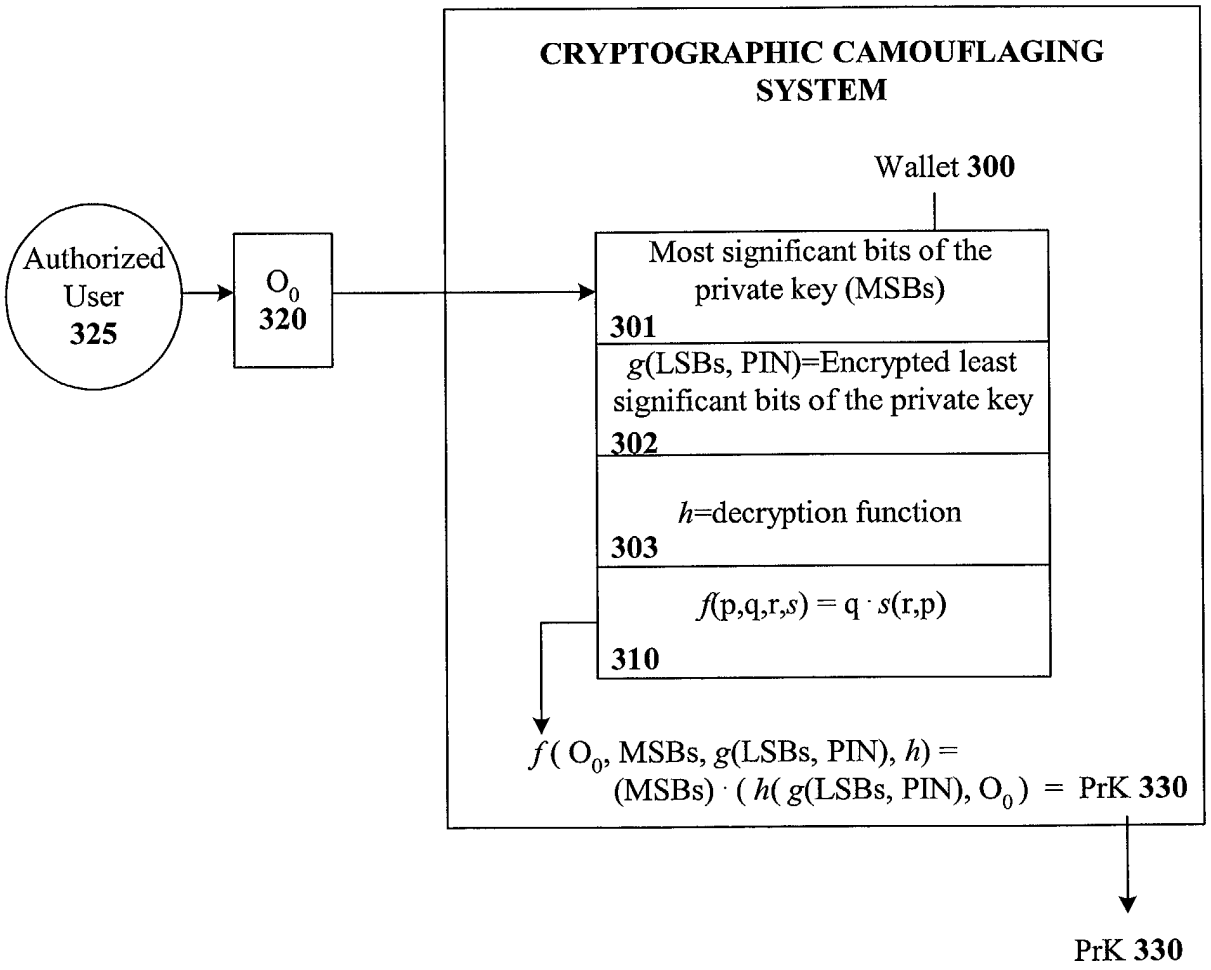

200
220
Encrypted Private Key
Decrypt
Decrypted Private Key
(PSEUDO-VALID PINS)
N:1 HASH
=?
STORED HASH
240
PIN
210

Figure 3


CRYPTOGRAPHIC CAMOUFLAGING SYSTEM
Wallet 300
Authorized User 325
O_0 320
Most significant bits of the private key (MSBs) 301
g(LSBs, PIN)=Encrypted least significant bits of the private key 302
h=decryption function 303
f(p,q,r,s) = q · s(r,p) 310
f(O_0, MSBs, g(LSBs, PIN), h) = (MSBs) · (h(g(LSBs, PIN), O_0) = PrK 330
PrK 330

TOOEOT" 206STOOT

Figure 4A

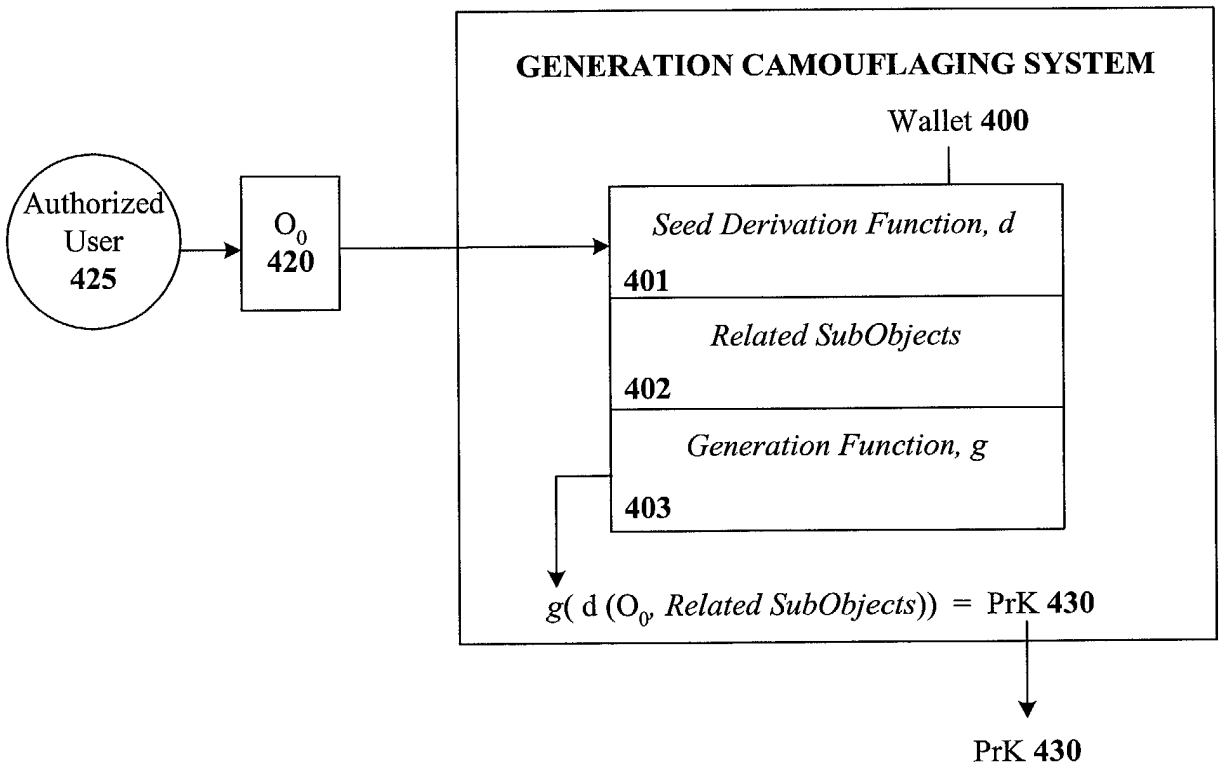


Figure 4B

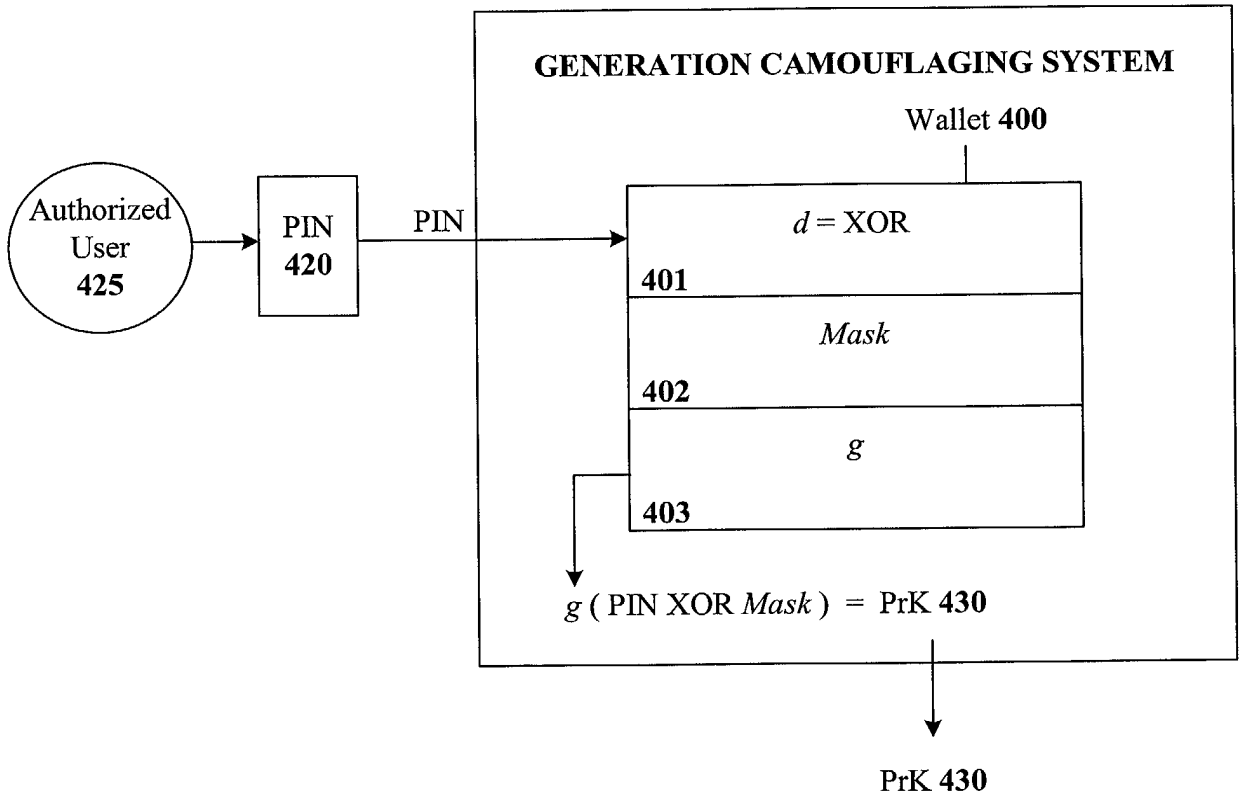
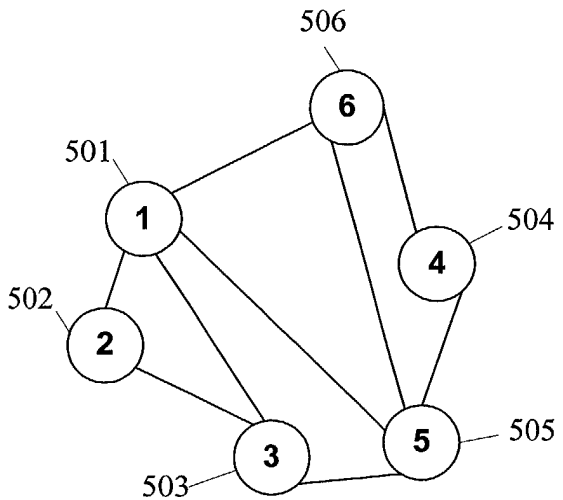

GENERATION CAMOUFLAGING SYSTEM
Wallet 400
Authorized User 425
PIN 420
PIN
d = XOR
401
Mask
402
g
403
g (PIN XOR Mask) = PrK 430
PrK 430

Figure 5

G 500

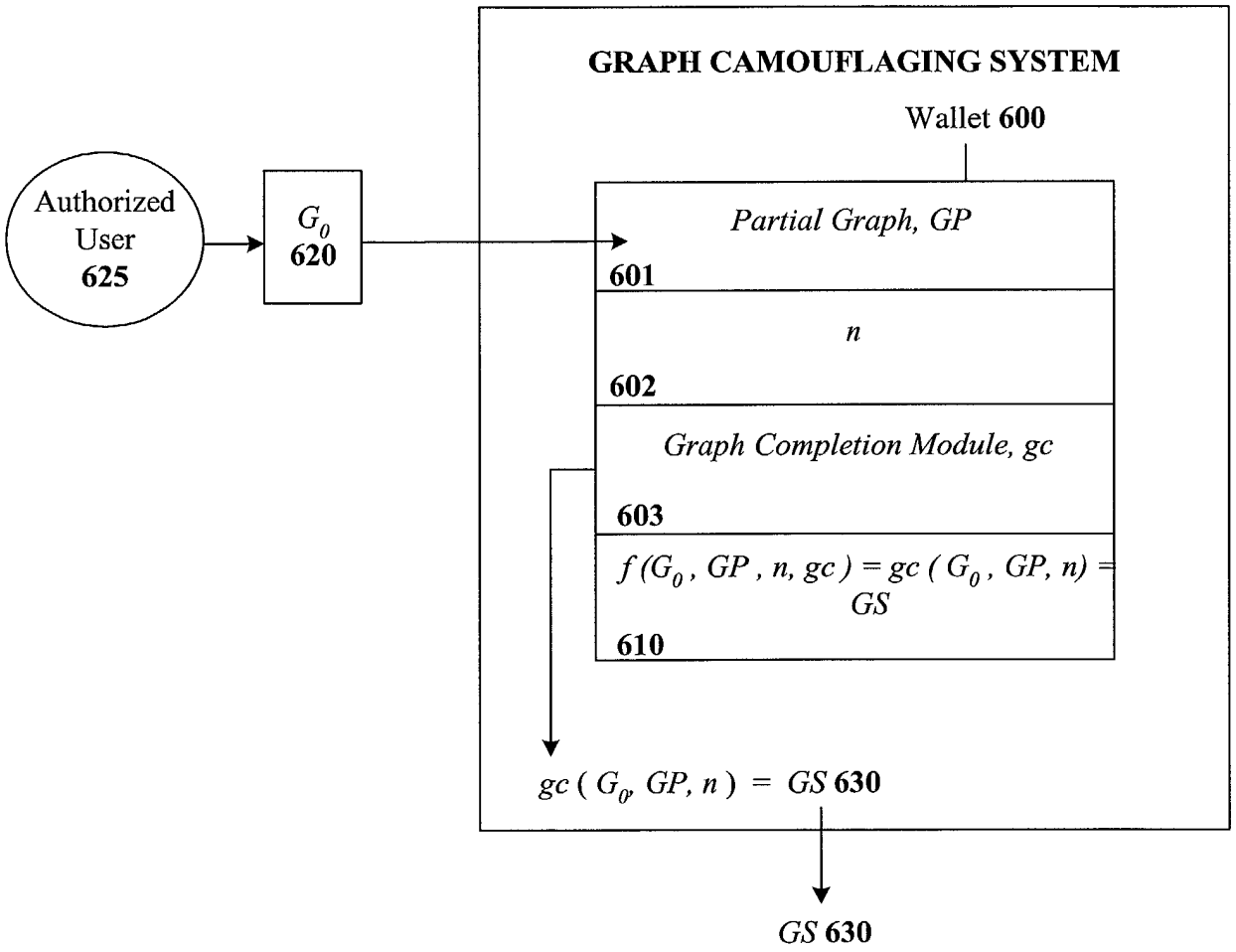


Adjacency Matrix M 510

501	502	503	504	505	506	
0	1	1	0	1	1	501
1	0	1	0	0	0	502
1	1	0	0	1	0	503
0	0	0	0	1	1	504
1	0	1	1	0	1	505
1	0	0	1	1	0	506

TOOSOT"206STOOT

Figure 6

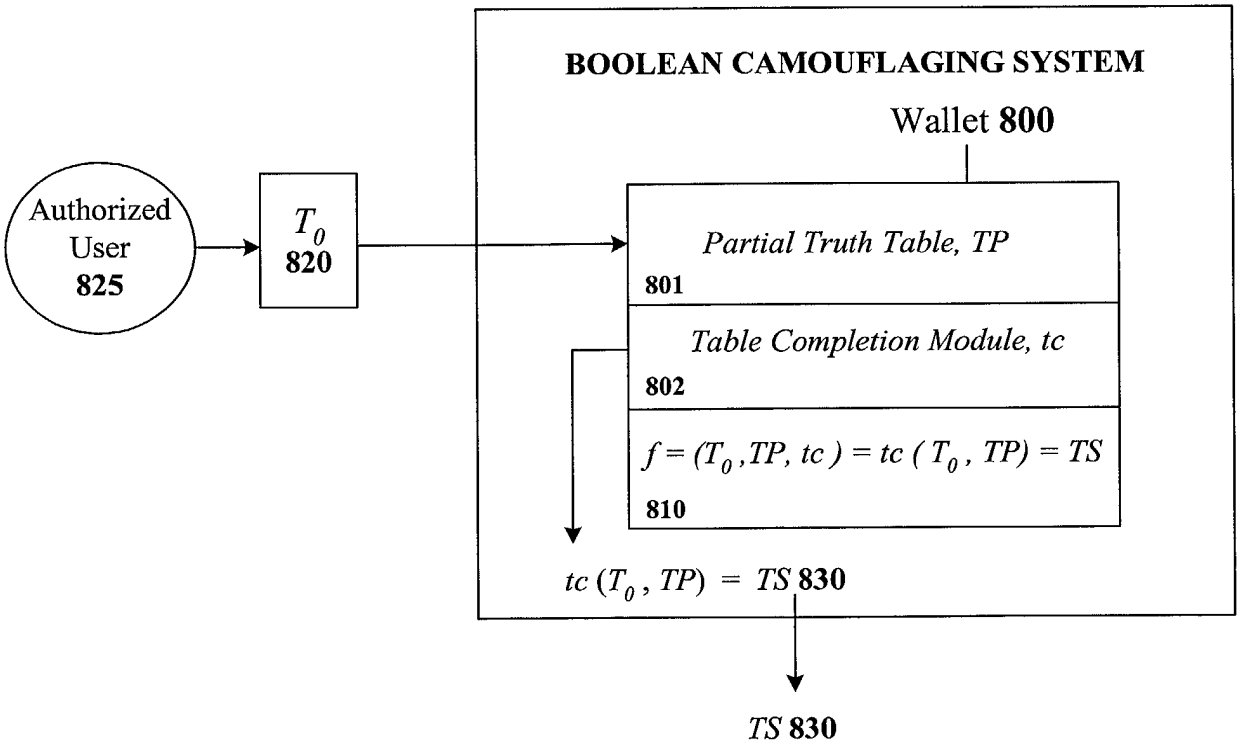


TODEOT" 206STOOT

Figure 7

x_1	x_2	x_3	x_4	**F**
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

Figure 8


BOOLEAN CAMOUFLAGING SYSTEM
Wallet 800
Authorized User 825
T_0 820
Partial Truth Table, TP
801
Table Completion Module, tc
802
$f = (T_0, TP, tc) = tc(T_0, TP) = TS$
810
$tc(T_0, TP) = TS$ 830
TS 830